

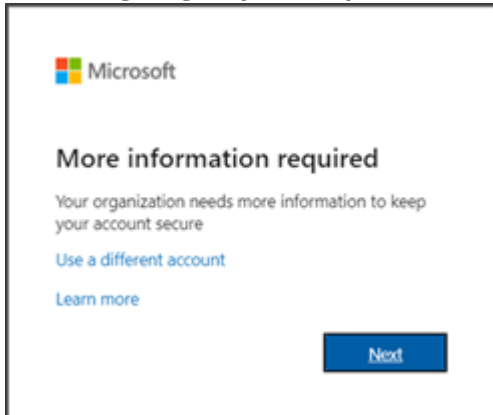
Multi-Factor Authentication (MFA)

This guide provides step-by-step instructions for users on how to reset their multi-factor authentication (MFA) using the Microsoft Authenticator app. It offers a user-friendly walkthrough, ensuring a seamless and secure process to regain access to their accounts while maintaining the highest level of security.

- [Setting Up Microsoft Authenticator](#)
- [MFA Passkeys](#)
- [Lost Phone / Can't Access Account](#)

Setting Up Microsoft Authenticator

When signing in you may see this message.



This message indicates that you must reconfigure your Multi-Factor Authentication. Follow through the on-screen prompts until you reach a page with a QR Code



Once you reach this page, please proceed to the next steps on your **mobile device**.



Delete previous sign-in method

This section is only necessary if you have **previously set up Microsoft Authenticator**.

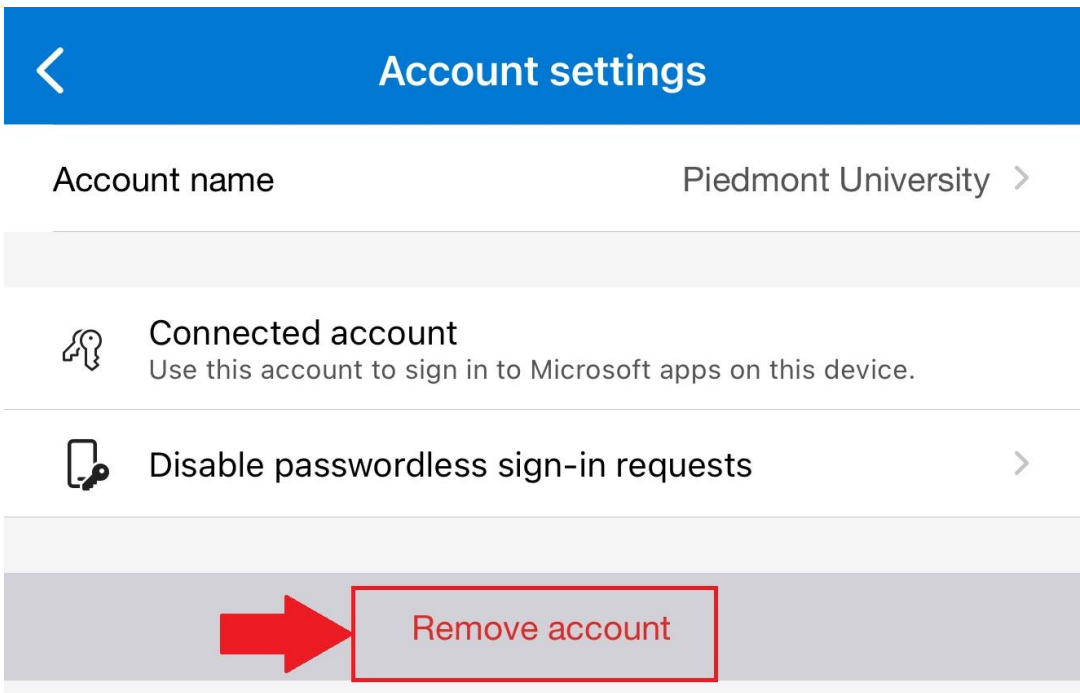
1. To set up MFA again you must **delete the previous account** to receive MFA notifications.
2. Open **Microsoft Authenticator**
3. Select your `@piedmont.edu` or `@lions.piedmont.edu` account



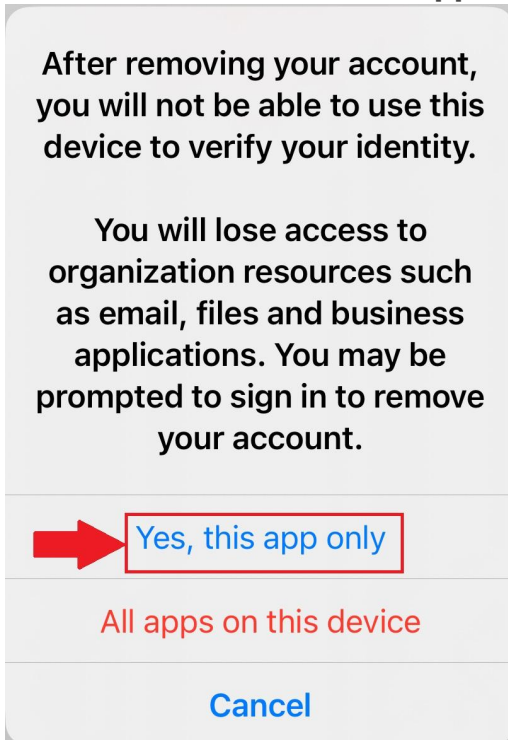
4. Select the **gear icon** in the top right corner



5. Select **Remove Account**



6. Press **Continue** and/or **This app only** to finish removing the account

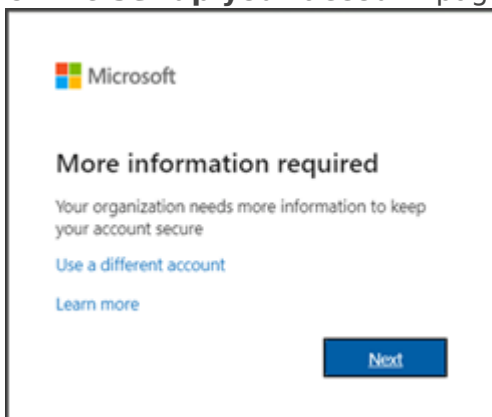


Set up Microsoft Authenticator

1. Open the **Microsoft Authenticator** app on your iOS or Android device
 - If you do not have Microsoft Authenticator installed, please download it from the **iOS App Store** or **Google Play Store**
2. Open the app, **allow notifications** (if prompted)
3. Select **Add account** from the '+' icon in the upper-right
4. Then select **Work or school account**

On your Computer:

5. On the **Set up your account** page, select **Next**



6. The **Scan the QR code** page appears



7. Use your mobile device to scan the **provided QR code** with the Microsoft Authenticator app
8. Select **Next** on your computer
9. A 2 digit number is displayed on the computer

On your Mobile Device:

9. A notification is sent to your mobile device prompting for a 2 digit number
10. On your mobile device, **enter the 2 digit number, show on the computer**, in the Microsoft Authenticator app
11. Select **Done** on your computer
12. Your security info is now updated to use the Microsoft Authenticator app by default to verify your identity when using two-step verification or password reset.

Our Helpdesk Team is happy to provide assistance with this process! Just give us a call at 706-894-4205!

Next Steps

Once you've set up Microsoft Authenticator, we recommend reviewing our documentation for Passkeys which you can find [here](#)!

Need Help?

If you encounter an error or need assistance with this guide, please contact the IT Department and include a screenshot with a brief description of the issue.













[**Contact the IT Department Here**](#)

MFA Passkeys

1. What is a Passkey?

A passkey is a modern, phishing-resistant way to sign in without using a password!

- Instead of something *you know* (like a password), a **passkey** uses something *you have* (your phone or device) and something *you are* (Face ID, Fingerprint, or device PIN)
- The credential is stored securely on your device and is never shared with the website or service that you're signing into. Because of this, passkeys can't be reused, stolen by fake websites, or guessed.
- Passkeys are based on industry security standards (FIDO2). Your device proves to Microsoft that it's really you, without ever sending a password across the internet.
 - If the site is not legitimate, the passkey simply won't work, and there's nothing for the attacker to steal.
- Your device becomes your key, and your identity stays locked inside it!

Bad  Password (Only)	Good  Password +	Better  Password +	Best Passwordless 
123456	 SMS	 Authenticator (Push notifications)	 Windows Hello
qwerty			
password	 Voice	 Software Tokens OTP	 Authenticator (Phone Sign-in)
iloveyou			
Password1		 Hardware Tokens OTP (Preview)	 FIDO2 security key

- Did you know that passwords are the weakest link in modern security? They are often:
 - Reused
 - Phished
 - Leaked in breaches
 - Guessed
- Microsoft's goal with passwordless sign-in is to:
 - **Eliminate passwords as an attack target** - No passwords means nothing to phish, reuse, or brute-force.
 - **Reduce account takeovers and phishing** - Passkeys only work on the real Microsoft sign-in and approved services. Fake sites can't trick your device into handing over a credential.

- **Make sign-ins faster and simpler** - Approving with Face ID, fingerprint, or a device PIN is quicker than typing passwords and codes.
- **Improve both security and user experience** - Stronger security without extra steps, fewer account lockouts.

Passkeys are part of Microsoft's move to a passwordless future where accounts are protected by your device and biometrics instead of passwords that can be stolen, guessed, or phished

2. Syncable Passkeys

A passkey lets you sign in without typing your password each time. It uses your device's built-in security, such as Face ID, fingerprint, screen lock, or device PIN.

We recommend saving your passkey to:

- Apple Passwords (if you use iPhone)
- Google Password Manager (if you use Android)

3. Before you Begin

Make sure you have:	Do not create a passkey on:
Your Piedmont email address	A public computer
Your current password	A shared family computer
You current MFA method	A classroom or lab computer
A personal phone or computer that only you use	A friend's phone

4. Enable Passkey Syncing (iOS/macOS)

1. Confirm your iCloud keychain is enabled
 - Open **Settings**
 - Select your Name / Apple ID at the top
 - Tap **iCloud**
 - Tap **Passwords and Keychain**
 - Confirm that the setting **Sync this iPhone** or **Sync this iPad** is enabled
 2. On Mac:
 - Open **System Settings**
 - Click your Apple Account
 - Click **iCloud**
 - Ensure **Passwords** is set to **Sync**
-

5. Create a Passkey

1. Open a web browser and visit <https://myaccount.microsoft.com>
 2. Expand **My Account**
 3. Select **Security Info**
 4. You will be prompted to login using MFA.
 5. Once logged in, select **Add sign-in method**
 6. Select **Passkey**
 7. Select **Next** and follow through the on-screen prompts
-

6. Sign in with Passkey

1. When you login using your Piedmont credentials, you will receive a new popup window in place of Microsoft Authenticator

PIEDMONT
UNIVERSITY

Face, fingerprint, PIN or security key

Your device will open a security window. Follow the instructions there to sign in.



Windows Security



Choose a passkey



iPhone, iPad, or Android device

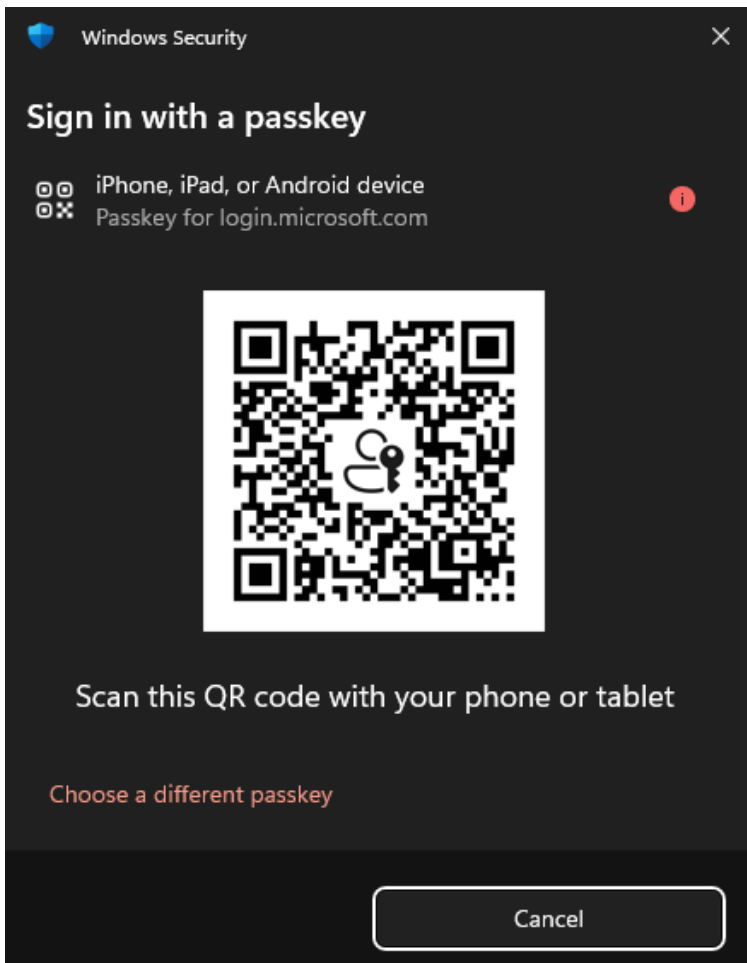


Security key

Cancel

2. Select **iPhone, iPad, or Android device**.

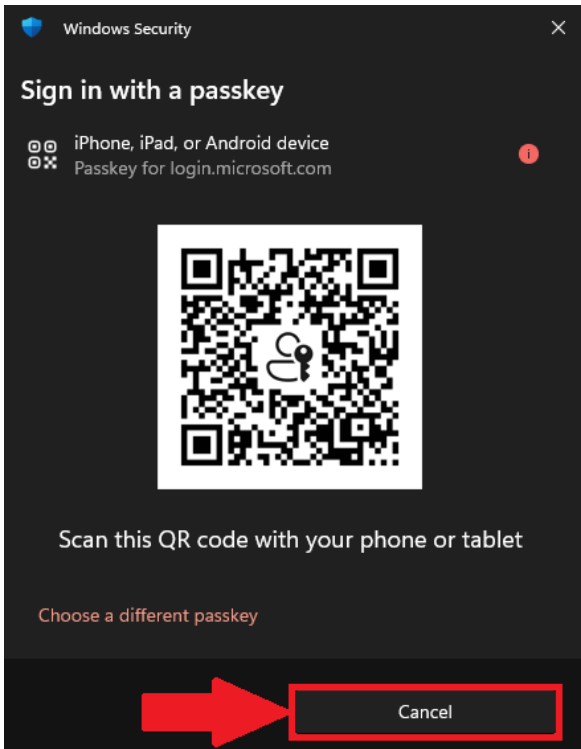
3. Use your mobile device to scan the QR Code on your computer, select **Sign in with Passkey**



4. On your mobile device, a message will appear "**Sign in to login.microsoft.com" on the other device with your passkey for "@piedmont.edu" saved in Passwords?**
 - Choose **Use Passkey**
5. Your mobile device will prompt for Face ID or biometrics.

7. Sign in using Microsoft Authenticator

1. In some cases you may need to use the original MFA through the Authenticator app, to do so, select the 'X' or 'Cancel' button and select **Sign in Another way**



PIEDMONT
UNIVERSITY

We couldn't sign you in

Something went wrong when trying to sign in with a passkey. Please try again.

[Learn more about passkeys](#)

Sign in another way

Back

Try again

2. Select **Approve a request on my Microsoft Authenticator app** to complete original MFA steps.



jeffersondavis@piedmont.edu

Verify your identity



Face, fingerprint, PIN or security key



Approve a request on my Microsoft Authenticator app



Use a verification code

[More information](#)

Are your verification methods current? Check at <https://aka.ms/mfasetup>

Cancel

3. Follow the on-screen instructions to approve the Authenticator request.

8. What happens when you get a new phone?

- If your passkey was saved to Apple Passwords or Google Password Manager, it may become available again after you:
 1. Sign into your new phone with the same Apple or Google account
 2. Enable iCloud Password or Google Password Manager sync
 3. Set up Face ID, fingerprint, screen lock, or device PIN
 4. Login to your Lions email using <https://www.office.com> or selfservice.piedmont.edu
 5. Select the saved passkey when prompted

If your passkey does not appear, you will need to [Contact IT](#) for assistance.

9. Security Notes

- Your passkey is only as secure as your Apple or Google account. Use a password manager!
 - Use a strong password on your Apple or Google account. Do not reuse passwords!
 - Keep account recovery options up to date on your Apple or Google account
 - Never share your phone PIN, Apple password, Google password, or Device unlock code
 - Do not save passkeys on shared or public devices
-

10. Next Steps

Review what you can do to help keep Piedmont secure [here](#)!

Need Help?

If you encounter an error or need assistance with this guide, please contact the IT Department and include a screenshot with a brief description of the issue.

[Contact the IT Department Here](#)

Lost Phone / Can't Access Account

1. Can't login due to MFA

If you lost or replaced your phone or no longer have access to your MFA method, you may not be able to Sign in to your Piedmont account.

This guide explains how to manage your sign in methods so that you can access your account.

- This guide is helpful when:
 1. You lost your phone
 2. You got a new phone
 3. Your phone was stolen
 4. Your phone was reset or wiped
 5. You deleted Microsoft Authenticator
 6. Microsoft Authenticator no longer show your Piedmont account
 7. You changed phone numbers
 8. You do not receive a text field to enter the 2-digit MFA number in Microsoft Authenticator
 9. You cannot access any of your sign-in methods

2. Manage your sign in Methods

You can only complete this section if you have access to at least 1 MFA method. (Passkey or Authenticator)

- You can add or remove MFA sign in methods by visiting <https://myaccount.microsoft.com> and logging in using your Piedmont email.
 1. Visit <https://myaccount.microsoft.com> and login using your Piedmont email
 2. In the left column, expand **My Account**
 3. Select **Security Info**
 4. You will be prompted to login using MFA

If you do not have access to your MFA method you will be required to contact the IT Department so that we may assist you.

5. Here you can manage your Sign-in Methods. If you got a new phone, you would need to delete the method labeled 'Microsoft Authenticator'.
6. Once deleted, select **Add Sign-in Method** and follow the on-screen instructions to add the Microsoft Authenticator App to your new device.
7. You can find instructions for setting up Microsoft Authenticator [here!](#)

3. Submit a Ticket to IT

If you cannot access your MFA methods you must submit a ticket to IT so that we may assist you in accessing your account again.

- When submitting a ticket, please include
 1. Your Full name
 2. Your Piedmont Email address
 3. a brief explanation of what happened
 4. Any screenshots of errors that you may receive.

Need Help?

If you encounter an error or need assistance with this guide, please contact the IT Department and include a screenshot with a brief description of the issue.

[Contact the IT Department Here](#)